UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/865,246	05/25/2001	Morton Gregory Swimmer	YOR920010310US1	3963

35526 7590 11/08/2005

DUKE. W. YEE
YEE & ASSOCIATES, P.C.
P.O. BOX 802333
DALLAS, TX 75380

EXAMINER	
ZAND, KAMBIZ	
ART UNIT	**PAPER NUMBER**
2132	

DATE MAILED: 11/08/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/865,246	SWIMMER ET AL.	
	Examiner	Art Unit	
	Kambiz Zand	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 August 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-67* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-67* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. The text of those sections of Title 35,U.S.Code not included in this section can be found in the prior office action.
2. The prior office actions are incorporated herein by reference. In particular, the observations with respect to claim language, and response to previously presented arguments.
3. Claims 13, 25, 38 and 59 have been amended.
4. Claims 1-67 are pending.

Response to Arguments

5. Applicant's arguments with respect to the claims have been considered but are moot in view of the new ground(s) of rejection.

As per applicant's arguments with respect to "journaled data", examiner refers applicant's to the definition given by applicant on page 3, lines 8-9 of the specification which is only restoration of the data to its original save data, common in mirroring storage art and as Cozza disclose on col.2, lines 49-67. Claims 13-67 are being rejected on 103 now rather than 102 rejections due to the amendment filed.

Claim Rejections - 35 USC § 103

6. **Claims 1-67** are rejected under 35 U.S.C. 103(a) as being unpatentable over Conklin et al (5,991,881 A) in view of Cozza (5,473,769 A).

As per claims 1, 22, 24, 26 and 47 Conklin et al (5,991,881 A) teach a system and a computer program product in a computer readable medium and a method in a data processing system for protecting data from damage, the system, the computer program product and the method comprising:

Jurnaling the data to from jurnaled data, wherein journaling the data comprises determining whether a virus is present in the data processing system after journaling of the data has began, including comparison and pattern matching (see abstract; fig.6 and associated text) but do not disclose restoring the data using the journaled data, maintaining a previous state of the data for subsequent, optional restore of the data to the previous state. However Cozza (5,473,769 A) disclose restoring the data using the journaled data, maintaining a previous state of the data for subsequent, optional restore of the data to the previous state (see col.2, lines 49-67). It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Cozza's restoration capability in Conklin's virus monitoring and detection method and system in order to eliminate the necessity of scanning all portions of files and volumes for all viruses (see col.2, lines 42-45).

As per claims 2, 27 and 48 Conklin et al (5,991,881 A) teach the system and the computer program product in a computer readable medium and the method of claims 1, 26 and 47 further comprising: responsive to an absence of an identification of the virus, discarding the journaled data (see fig.6 and 7 and associated text with respect to

discard).

As per claims 3, 28 and 49 Conklin et al (5,991,881 A) teach the system and the computer program product in a computer readable medium and the method of claims 1, 26 and 47, wherein the determining step comprises: performing pattern matching (see fig.7 and associated text).

As per claims 4, 29 and 50 Conklin et al (5,991,881 A) teach the system and the computer program product in a computer readable medium and the method of claims 3, 28 and 49, wherein the performing step includes: comparing a set of actions occurring within the data processing system with a set of patterns (see fig.7 and associated text).

As per claims 5, 30 and 51 Conklin et al (5,991,881 A) teach the system and the computer program product in a computer readable medium and the method of claims 1, 26 and 47, wherein the data is located in a storage device external to the data processing system (see fig.3, 4 and associated text where the storage within the hosts are external to monitoring system).

As per claims 6, 31 and 52 Conklin et al (5,991,881 A) teach the system and the computer program product in a computer readable medium and the method of claims 1, 26 and 47, further comprising: recording a sequence of actions occurring within the data processing system (see fig.4, evidence log; fig.8 and associated text).

As per claims 7, 32 and 53 Conklin et al (5,991,881 A) teach the system and the computer program product in a computer readable medium and the method of claims 1, 26 and 47, wherein the data is data accessed by a process within the data processing system (see fig.4-5 and associated text).

As per claims 8, 33 and 54 Conklin et al (5,991,881 A) teach the system and the computer program product in a computer readable medium and the method of claims 1, 26 and 47 further comprising: responsive to an identification of the virus, blocking access to the data by a process accessing the data (see col.5, lines 34-38).

As per claims 9, 34 and 55 Conklin et al (5,991,881 A) teach the system and the computer program product in a computer readable medium and the method of claims 1, 26 and 47 further comprising: responsive to an identification of the virus, generating an indication halting a process accessing the data (see col.5, lines 24-44).

As per claims 10, 35 and 56 Conklin et al (5,991,881 A) teach the system and the computer program product in a computer readable medium and the method of claims 1, 26 and 47, wherein the data journaled is data accessed by a single process and maintained until a determination is made that the single process is eliminated as a virus candidate (see fig.6 and associated text).

As per claims 11, 36 and 57 Conklin et al (5,991,881 A) teach the system and the computer program product in a computer readable medium and the method of claims 1, 26 and 47, wherein the journaled data is stored in a protected memory accessible only by the method (see fig.9 and associated text).

As per claims 12, 37 and 58 Conklin et al (5,991,881 A) teach the system and the computer program product in a computer readable medium and the method of claims 11, 37 and 57, wherein the journaled data is stored in a data structure located in a protected memory inaccessible by a process (see fig.5 and associated text).

As per claims 13, 25, 38 and 59 Conklin et al (5,991,881 A) teach a system and a computer program product in a computer readable medium and a method, the system, the computer program product in a computer readable medium and the method comprising: saving a state of a data object in response to a request to access the data object by a process; performing pattern matching of a set of actions taken within the data processing system; and determining whether an unauthorized intrusion has occurred in response to performing pattern matching (see fig.6-9 and associated text where base on request , detection, pattern matching are taken to determine an attack or intrusion) but do not disclose initiation a rollback to return the data object back to its saved state. However Cozza (5,473,769 A) disclose restoring the data using the journaled data, maintaining a previous state of the data for subsequent, optional restore of the data to the previous state (see col.2, lines 49-67). It would have been obvious to

one of ordinary skilled in the art at the time the invention was made to utilize Cozza's restoration capability in Conklin's virus monitoring and detection method and system in order to eliminate the necessity of scanning all portions of files and volumes for all viruses (see col.2, lines 42-45).

As per claims 14, 39 and 60 Conklin et al (5,991,881 A) teach the system and the computer program product in a computer readable medium and the method of claims 13, 38 and 59, wherein the performing step comprises: comparing the set of actions to a pattern from a set of patterns to form a comparison; determining whether the comparison indicates that the unauthorized intrusion has occurred; and responsive to an absence of the unauthorized intrusion, repeating the comparing step using another pattern from the set of patterns (see fig.6-9 and associated text).

As per claims 15, 40 and 61 Conklin et al (5,991,881 A) teach the system and the computer program product in a computer readable medium and the method of claims 13, 38 and 59, wherein the performing step comprises: matching patterns with the set of actions; determining whether the unauthorized intrusion has occurred; if an intrusion is absent, determining whether a time threshold has been reached; and if an absence of a reaching of the time threshold is present, repeating the matching step using another set of actions (see fig.6-8 and associated text; col.6, lines 60-63).

As per claims 16, 41 and 62 Conklin et al (5,991,881 A) teach the system and the

computer program product in a computer readable medium and the method of claims 14, 39 and 60, wherein match between the pattern and the set of actions identifies an absence of the unauthorized intrusion (see fig.6, discard).

As per claims 17, 42 and 63 Conklin et al (5,991,881 A) teach the system and the computer program product in a computer readable medium and the method of claims 14, 39 and 60, wherein match between the pattern and the set of actions identifies a presence of the unauthorized intrusion (see fig.6-9).

As per claims 18, 43 and 64 Conklin et al (5,991,881 A) teach the system and the computer program product in a computer readable medium and the method of claims 13, 38 and 59, wherein the intrusion is caused by a virus (see abstract; fig.6).

As per claims 19, 44 and 65 Conklin et al (5,991,881 A) teach the system and the computer program product in a computer readable medium and the method of claims 13, 38 and 59, wherein the intrusion is caused by an authorized user input (see col.6, lines 47-55 where all addresses of the intrusion are recorded, Examiner considers the addresses includes both authorized or non authorized).

As per claims 20, 45 and 66 Conklin et al (5,991,881 A) teach the system and the computer program product in a computer readable medium and the method of claims

13, 38 and 59 further comprising: saving a state of all data objects within the data processing system (see fig.8 with respect to logs and associated text).

As per claims 21, 46 and 67 Conklin et al (5,991,881 A) teach the system and the computer program product in a computer readable medium and the method of claims 13, 38, and 59, wherein the data is located in a storage device external to the data processing system (see fig.3, 4 and associated text where the storage within the hosts are external to monitoring system).

As per claim 23 Conklin et al (5,991,881 A) teach all limitation of the claims but do not disclose, wherein the intrusion protection system is located within an operating system. However it would have been obvious to one of ordinary skilled in the art that operating system is just another program type and such instructions within a program as applied above is also could be implemented within an operating system as another part of the program.

Conclusion

7. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kambiz Zand whose telephone number is (571) 272-3811. The examiner can normally reached on Monday-Thursday (8:00-5:00). If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone numbers for the organization where this application or proceeding is assigned as (571) 272-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private

PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Kambiz Zand

11/04/2005

AU 2132